HEOS Fleet — Privacy Policy

Yantralive Parts Technology Pvt. Ltd.

Effective: 27 April 2026 · Last updated: 27 April 2026

1. About this policy

This Privacy Policy describes how Yantralive Parts Technology Pvt. Ltd. ("Yantralive," "we," "us," or "our") collects, uses, stores, shares, and protects information when you use the HEOS Fleet mobile application and the associated web application (together, the "HEOS Fleet Service" or the "Service").

HEOS Fleet is a business-to-business fleet and equipment management platform. The Service is provided to construction-equipment owners, fleet operators, and rental companies (each, a "Customer"), and used by their employees and authorised personnel (operators, supervisors, fleet managers, back-office staff, and owners) in the course of the Customer's business.

This policy applies to all users of the Service and is written to comply with the Digital Personal Data Protection Act, 2023 ("DPDP Act") of India and applicable principles of fair information practice in the jurisdictions where HEOS Fleet is used. Where you are an employee or authorised user of a Customer, your employer's own privacy and employment policies may also apply to your use of the Service in addition to this policy.

2. Who we are

Data Fiduciary: Yantralive Parts Technology Pvt. Ltd.

Registered office: Bengaluru, Karnataka, India.

Contact: privacy@yantralive.com

Grievance Officer: [Name to be designated], reachable at grievance@yantralive.com. Under the DPDP Act, the Grievance Officer is the point of contact for any concern regarding the processing of your personal data, and will respond within the timelines prescribed by law.

3. Information we collect

We collect the following categories of information when you use the Service. Not every category applies to every user; what we collect depends on your role and how your Customer has configured the Service.

3.1 Identity and account information

- Mobile number (used for one-time-password authentication; we do not use passwords)
- Name and, where provided by your Customer, email address

- Role assigned by your Customer (Owner, Fleet Manager, Site Supervisor, Operator, Technician, Back-office, etc.) and any associated designation
- Site and machine assignments within your Customer's organisation

3.2 Operational and work data

HEOS Fleet exists to help your Customer manage equipment and field operations. In the course of normal use, the Service records:

- Hour-meter (HMR) readings you enter or that are read from connected IoT devices
- Fuel logs, including fuel quantity, cost, vendor, and any associated receipt photo
- Attendance check-ins and check-outs, including timestamp and shift information
- Expense entries you submit for approval
- Equipment inspections, including answers to checklist items, photos of flagged items, and operator signatures
- Fuel requests, approvals, and any associated workflow state
- Compliance documents you upload on behalf of your Customer (e.g., insurance, registration)

3.3 Location information

With your permission, the Service collects precise device location (GPS) in the following situations:

- When you check in or check out for attendance, to verify the action against your Customer's site geofence
- When you ask the voice agent for the location of a machine, only to satisfy that query
- When you submit work that is location-tagged by your Customer's configuration (for example, a fuel log tied to a specific site)

You can change or revoke location permission at any time using your device's system settings. Some features (notably attendance check-in within a geofenced site) will not function without location access.

3.4 Voice and audio data

HEOS Fleet includes a voice agent that lets you speak commands in English, Hindi, Kannada, and other supported languages. When you use this feature:

- Your microphone records audio only while you press and hold the voice button. We do not record continuously or in the background.
- The recorded audio is sent to Sarvam AI to convert your speech into text (this step is necessary; without it, the voice agent cannot understand you).

- The resulting text is sent to Anthropic (the maker of the Claude AI model) to determine what action you intend (this step is also necessary).
- If your intent is clear, the action is recorded against the appropriate machine, site, or work record. If clarification is needed, the agent asks a follow-up question.

How long we keep the resulting transcript, and the choices available to you and your Customer, are described in detail in Section 6 below.

3.5 Photos and images

With your permission, the Service uses your device camera to capture:

- Photos of fuel receipts, which are sent to Anthropic for automated reading (OCR) of the receipt fields, then attached to the corresponding fuel log
- Photos of inspection findings (for example, a damaged tyre flagged during a daily check)
- Optional photos of machines, sites, or other work artefacts

These images are stored in encrypted cloud storage in India (Amazon S3, Mumbai region).

3.6 Machine and IoT telemetry

Where your Customer has equipped a machine with a supported IoT telemetry device (for example, an Omnicomm tracker), HEOS Fleet retrieves the following data from the device or the device's vendor: GPS coordinates, engine running hours, fuel level and consumption, voltage, ignition events, and similar machine-state signals. This data describes the machine, but it can indirectly reflect the activity of an operator assigned to that machine.

3.7 Technical and device information

To keep the Service reliable and to investigate problems, we collect:

- Application version, device operating system version, and device model
- Crash reports and error events (via Sentry, see Section 5). Mobile numbers contained in any error context are masked to the last four digits before transmission. Authentication tokens are removed before transmission.
- Standard server logs of API requests, including time, endpoint, response code, and the user account making the request

4. How we use this information

We use the information described above for the following purposes:

- Provide the Service: log work, track machines, run inspections, manage attendance, calculate cost and utilisation, and the other features your Customer has subscribed to.
- Authenticate you and protect your account against unauthorised access.

- Enforce site geofences, shift assignments, and approval workflows configured by your Customer.
- Operate the voice agent (speech-to-text, intent recognition, action execution).
- Provide customer support to your Customer's administrators and to you, where you contact us directly.
- Investigate errors, debug issues, and improve the quality and reliability of the Service.
- Comply with applicable law and respond to lawful requests from authorities.

We do not use your personal data for advertising. We do not sell your personal data.

5. Third-party service providers

We rely on a small set of trusted service providers to operate HEOS Fleet. Each is bound by contractual obligations to handle your data only for the purposes for which we engage them.

Sarvam AI (India)

Used for converting speech to text in Indian languages. Receives the audio segment captured during a voice command and returns transcribed text.

Anthropic (United States)

Provides the Claude AI model used for understanding voice intents and for reading fuel-receipt photos (optical character recognition). Receives the transcript text or the receipt image and returns a structured result. Your data is processed transiently to produce the result; per Anthropic's commercial terms, your inputs and outputs are not used to train Anthropic's models.

Amazon Web Services (Mumbai region, India)

Hosts our application servers, our PostgreSQL database, and our object storage. All Customer data, photos, voice transcripts (where retained), and operational records are stored in the Mumbai region ("ap-south-1").

Sentry (European Union)

Receives application crash reports and error events to help us identify and fix bugs. Personally identifying values such as mobile numbers and authentication tokens are scrubbed before transmission. Sentry stores this data on servers in the European Union.

MSG91 (India)

Sends one-time passwords to your mobile number for authentication. Receives only your mobile number and the OTP, both for the limited purpose of delivering the message.

Omnicomm and similar IoT telemetry vendors

Where your Customer's machines are equipped with a supported telemetry device, the device vendor (such as Omnicomm) is the source of machine telemetry. The vendor's own privacy and data-handling terms apply to the data the device generates before it reaches HEOS Fleet.

Google Play Services and Apple App Store

As mobile platforms, Google and Apple receive standard app-distribution and crash-related data per their own published policies.

6. Voice transcript retention and your choice

This section explains a specific choice your Customer's administrator has about voice data, because the choice meaningfully affects what is stored.

Two distinct things happen when you use the voice agent

Processing (always required, cannot be disabled). To understand what you said and act on it, the audio you record must pass through Sarvam AI (speech-to-text) and the resulting text must pass through Anthropic (intent recognition). Without these two steps, the voice agent cannot function. This processing is transient: the audio and the text exist in the third parties' systems only long enough to produce a result, after which they are discarded according to those providers' terms.

Retention (configurable by your Customer). Separately, HEOS Fleet by default stores the resulting transcript text alongside the work record it produced (for example, the HMR log entry created by the voice command). Retention helps us investigate issues, support your Customer's administrators, and improve the Service. This retention is the part your Customer's administrator can turn off.

How the choice works

- By default, voice transcript retention is ON for production Customers. Each retained transcript is stored in our database in the Mumbai region, linked to the work record it produced and to the user who created it.
- Your Customer's administrator can switch retention OFF at any time via Company Settings in the Service. The change takes effect immediately on subsequent voice commands; you do not need to log out and back in for it to apply. Once OFF, new transcripts are not stored.
- Switching retention OFF is forward-looking. Transcripts already retained at the moment of the change remain in our database under the security and retention controls described elsewhere in this policy. If you or your Customer want existing retained transcripts deleted, you may request deletion using the contact details in Section 14; we will action lawful requests within the timelines required by law.

- Voice features continue to work whether retention is ON or OFF. Only the storage of transcripts changes.

7. Where your data is stored

All Customer data created in the Service — including identity records, operational records, location data, retained voice transcripts, photos, and IoT telemetry — is stored on Amazon Web Services infrastructure in the Mumbai region (ap-south-1), India.

Limited categories of data are processed outside India by the third-party providers listed in Section 5: speech and intent processing by Anthropic in the United States; receipt OCR by Anthropic in the United States; crash and error events by Sentry in the European Union. Each transfer is for the specific purpose stated and is governed by the contractual terms we have in place with the provider.

8. How we protect your data

- Network traffic between your device and our servers, and between our servers and our service providers, is encrypted in transit using TLS.
- Stored data is protected by AWS-managed encryption at rest for our database and for our object storage.
- Access to production systems is restricted to authorised Yantralive personnel and is logged.
- Authentication uses one-time passwords delivered to your registered mobile number; we do not store passwords.
- We use the principle of least privilege: each user can see only the data their role and assignment within their Customer's organisation entitles them to see.
- We monitor the Service for errors and anomalies and act on what we find.

No system can be guaranteed to be fully secure. We will notify your Customer of any security incident affecting their data within the timelines required by applicable law.

9. How long we keep your data

In general, we retain Customer data for the duration of your Customer's subscription to the Service, plus a reasonable period afterwards to allow for export, dispute resolution, and compliance with legal obligations. Specifically:

- Operational records (HMR, fuel, attendance, expenses, inspections) are retained for the life of the Customer account, because these records form the Customer's own business history.
- Voice transcripts, where retained per Section 6, follow the same retention as the operational record they belong to.

- Photos are retained for the life of the Customer account.
- Authentication and audit logs are retained for at least 12 months for security investigation purposes, longer where required by law.
- Crash and error events held by Sentry are retained per Sentry's standard retention (typically 90 days for events).

On termination of a Customer's subscription, we will, on written request from the Customer's authorised contact, return or delete Customer data within a reasonable period, subject to any legal hold or retention requirement.

10. Sharing and disclosure

We share personal data only as follows:

- With the Customer that has authorised your use of the Service. Your Customer can, through their administrators, see the data you create in the Service in the course of their business.
- With the third-party service providers listed in Section 5, only for the purposes described.
- With law enforcement, regulators, or other authorities where we are legally compelled to do so, and only to the extent of the legal compulsion.
- With professional advisors (lawyers, accountants, auditors) bound by confidentiality, where reasonably necessary.
- In connection with a corporate transaction such as a merger or acquisition, in which case we will require the receiving party to honour this policy.

We do not sell personal data. We do not use personal data for behavioural advertising.

11. Your rights

Subject to the DPDP Act and other applicable laws, you have the following rights with respect to your personal data:

- Right to access: you can ask what personal data we hold about you.
- Right to correction and completion: you can ask us to correct inaccurate or incomplete data.
- Right to erasure: you can ask us to delete your personal data, subject to legitimate retention obligations and to your Customer's legitimate business interest in records you created in the course of your work.
- Right to grievance redressal: you can raise a complaint with our Grievance Officer (see Section 2).
- Right to nominate: you can nominate another individual to exercise these rights on your behalf in the event of your death or incapacity.

To exercise these rights, write to us at privacy@yantralive.com. We will verify your identity before responding and will respond within the timelines required by law.

If you are an employee or authorised user of a Customer, please note that some requests — particularly erasure of operational records you created on behalf of your employer — may need to be directed to your Customer, who is the controlling party for the data created in the course of their business.

12. Children's privacy

HEOS Fleet is a workplace tool intended for adult professionals operating in the construction equipment and fleet management industry. The Service is not directed at children. We do not knowingly collect personal data from children. If we learn that we have inadvertently done so, we will delete it.

13. Changes to this policy

We may update this policy from time to time to reflect changes in the Service, in our practices, or in the law. When we make a material change, we will update the "Last updated" date at the top of this policy and, where appropriate, notify your Customer's administrator and prompt you to review the change inside the Service. The version posted at https://yantralive.com/heos-fleet/privacy-policy is always the current version.

14. Contact us

Questions, requests under Section 11, or general feedback on this policy:

Email: privacy@yantralive.com

Grievance Officer: grievance@yantralive.com

Postal address: Yantralive Parts Technology Pvt. Ltd., Bengaluru, Karnataka, India.

If you are an end user, you may also contact your Customer's administrator with questions about how your employer uses HEOS Fleet.